ESET ENDPOINT SECURITY for ANDROID

User Guide

(intended for product version 2.0 and higher)

Click here to download the most recent version of this document

ESET ENDPOINT SECURITY

Customer Care: www.eset.com/support

REV. 03.01.2017

Contents

1. Introduction

The new generation of ESET Endpoint Security for Android (EESA) is designed to work with ESET Remote Administrator (ERA) 6, the new management console which allows for remote management of all ESET security solutions. ESET Endpoint Security for Android 2 is only compatible with ERA 6 and later.

ESET Endpoint Security for Android is designed to protect corporate mobile devices against the most recent malware threats and secure your data even if your device is lost or stolen. It also helps system administrators keep their devices in compliance with company security policies.

ESET Endpoint Security can be also applied in small-to-medium sized companies without the need of remote management via ESET Remote Administrator. IT technician, system administrator or the actual Endpoint user can simply share his ESET Endpoint Security configuration with other colleagues. This process completely diminishes the need of product activation and manual setup of each product module otherwise required right after the installation of ESET Endpoint Security.

1.1 What's new in version 2

Application Control

Application Control allows administrators to monitor installed applications, block access to defined applications and lower the risk of exposure by prompting users to uninstall certain applications. See the Application Control section of this guide for more info.

Device Security

Device security allows administrators to execute basic security policies across multiple mobile devices. For example, the administrator can:

- set the minimum security level and complexity of screen lock codes
- set maximum number of failed unlock attempts
- set the duration after which users must change their screen lock code
- set the lock screen timer
- restrict camera usage

See the Device Security section of this guide for more info.

Import and export of settings

To easily share settings from one mobile device with another if the devices are not managed by ERA, ESET Endpoint Security 2 introduces the option to export and import program settings. The administrator can manually export device settings to a file which can then be shared (for example, via email) and imported to any device running the client application. When the user accepts the received settings file, it automatically defines all settings and activates the application (provided the license information was included). All settings are protected by the administrator password.

Anti-Phishing

This feature protects users from accessing malicious web sites when using supported web browsers (default Android browser and Chrome).

Anti-Phishing technology protects users from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites impersonating legitimate ones. When a device attempts to access a URL, ESET Anti-Phishing compares it against the ESET database of known phishing sites. If a match is found, connection to the URL is aborted and a warning message is displayed.

Notification center

ESET Endpoint Security provides users with one unified notification center where they can find all notifications regarding application features that require their attention. Notification center will provide information about various events, the reasons why they are not compliant with company policies and what should be done to fulfill these requirements. Notifications are organized according to priority, with higher priority notifications displayed at the top of the list.

New licensing system

ESET Endpoint Security fully supports ESET License Administrator – the new licensing model introduced with ESET Remote Administrator 6.

A new licensing framework simplifies the deployment and long-term usage of ESET security software. When the customer requests a change to their license, the change is automatically and transparently reflected in all products using the license. This allows customers to use their email address and a custom password as credentials, rather than the ESET-issued Username and Password used by older products.

The introduction of license keys and automatic license updates (upon renewal or any other license operation), means customers can be sure that they are protected. The ESET License Administrator portal and the ability to assign license authorization rights by email address (based on the customers account information) simplify license management and deployment. Using ESET License Administrator, license owners can delegate license management to a responsible entity (even a third party, without losing a control over the license).

Managed upgrade of a product to a newer build

Systems administrators using ERA who do not want to upgrade ESET Endpoint Security for Android to the latest version as soon as it becomes available have the option to control the update mechanism.

Setup wizards

ESET Endpoint Security offers post-installation Setup Wizards for selected features to make the process more straightforward.

Improved Antivirus

- Improved Real-time (On-access) scan times
- Integrated ESET Live Grid
- 2 levels of scanning—Smart and In-depth
- On-demand scanner enhancements—background scanning, pause scan
- Scheduled scanning—a full-device scan can be scheduled by the administrator
- On-charger scan—a scan will start automatically when the device is in an idle state (fully charged and connected to a charger)
- Enhanced virus database update configuration – the administrator can specify the timing of regular updates and select the update server that devices use (release server, pre-release server, local mirror)

Detailed logs with scan results are sent to ERA. ESET Endpoint Security includes features from ESET Endpoint Security version 1, like detection of potentially unsafe applications, detection of potentially unwanted applications and USSD Control.

Improved SMS & Call Filter

SMS & Call Filter, previously known as Antispam, protects users from unwanted calls, SMS and MMS messages. This feature now offers two types of rules: administrator rules and user rules, where admin rules are always superior.

Other improvements include:

- Time-based blocking – the user or administrator can block calls and messages received during their specified times
- One-touch blocking for the last caller or message sender, phone number, contacts group, hidden or unknown numbers

Improved Anti-Theft

Anti-Theft features allow administrators to protect and locate a device if it is lost or stolen. Anti-Theft measures can be triggered from ERA, or via Remote commands.

ESET Endpoint Security 2 uses the same Remote commands from version 1 (**Lock**, **Wipe** and **Find**). The following entirely new commands have been added:

- **Unlock**—unlocks the locked device
- **Enhanced Factory reset**—all accessible data on the device will be quickly removed (file headers will be destroyed) and the device will be reset to its default factory settings
- **Siren**—the lost device will be locked and it will play a very loud sound even if the device is set to mute

To strengthen the security of Remote commands, the administrator will receive a unique and time-limited verification SMS code on his mobile phone (at the number defined in the Admin contacts list) when he executes a Remote command. This verification code will be used to verify a particular command.

Anti-Theft commands from ERA

Anti-Theft commands can now be performed from ERA as well. The new mobile device management functionality allows the administrator to send Anti-Theft commands in just a few clicks. Tasks are immediately submitted for execution via the Mobile Device Connector component that is now a part of ERA infrastructure.

Admin Contacts

This is the List of administrator phone numbers protected by the admin password. Anti-Theft commands can only be sent from trusted numbers.

Display message from ERA

When managing devices remotely, the administrator can send a custom message to a particular device or a group of devices. This helps to communicate an urgent message to the users of managed devices. The message will be displayed in a form of a pop-up, so the user will not miss it.

Lock screen custom information

The administrator is able to define custom information (company name, email address, message) which will be displayed when the device is locked, with the option to call one of the pre-defined admin contacts.

Improved remote management with ESET Remote Administrator 6

It is now possible to configure and set all application settings via remote policy, from Antivirus, SMS & Call filter and Device Security settings to Application Control restrictions, etc. This allows administrators to enforce company security policy on the entire network, including mobile devices.

ESET Endpoint Security for Android version 2 offers much improved reporting visible from ERA Web Console. This allows administrators to promptly identify problematic devices and find the source of the problem.

Management of Android devices is now an integral part of ESET Remote Administrator 6 with nearly all of the same functions available for ESET desktop products like ESET Endpoint Antivirus 6 and ESET Endpoint Security 6.

Local administration

ESET Endpoint Security for Android provides administrators with the option to setup and manage endpoints locally if they choose not to use ESET Remote Administrator. All application settings are protected by Admin password so the application is under full control at all times.

Improved distribution and installation of the product

In addition to traditional installation methods (download and install a package from ESET website, distribute the installation package via email), administrators and users have the option to download and install the application from the Google Play store.

Improved activation of the product

After download and installation, the administrator or user has several options to activate the product:

- They can utilize the new licensing options and manually enter the License key or Security admin account.
- They can click on the link sent in an email from the administrator. The product will configure ERA connection automatically and license information will be pushed to the device from ERA.
- The administrator can manually enter ERA connection information.
- Importing the file containing the application settings (with the license information included) will subsequently activate the application.

Improved identification of the mobile device in ERA

During the enrollment process, Android devices are whitelisted, so that only authorized devices can connect to ERA. This improves security and also simplifies individual device identification—each mobile device is identified by its name, description and IMEI. WiFi only devices are identified by their WiFi MAC address.

Redesigned Graphic User Interface

ESET Endpoint Security delivers an enhanced user experience similar to the one featured across all ESET solutions for business customers.

Ease of use

Thanks to the new user interface the product is easier to navigate and use. The structure of the GUI matches the new generation of ESET Endpoint solutions and ESET Remote Administrator.

1.2 Minimum system requirements

To install ESET Endpoint Security, your Android device must meet the following minimum system requirements:

- Operating system: Android 4 (Ice Cream Sandwich) and later
- Touchscreen resolution: 480x800 px
- CPU: ARM with ARMv7 instruction set, x86 Intel Atom
- Free storage space: 20 MB
- Internet connection

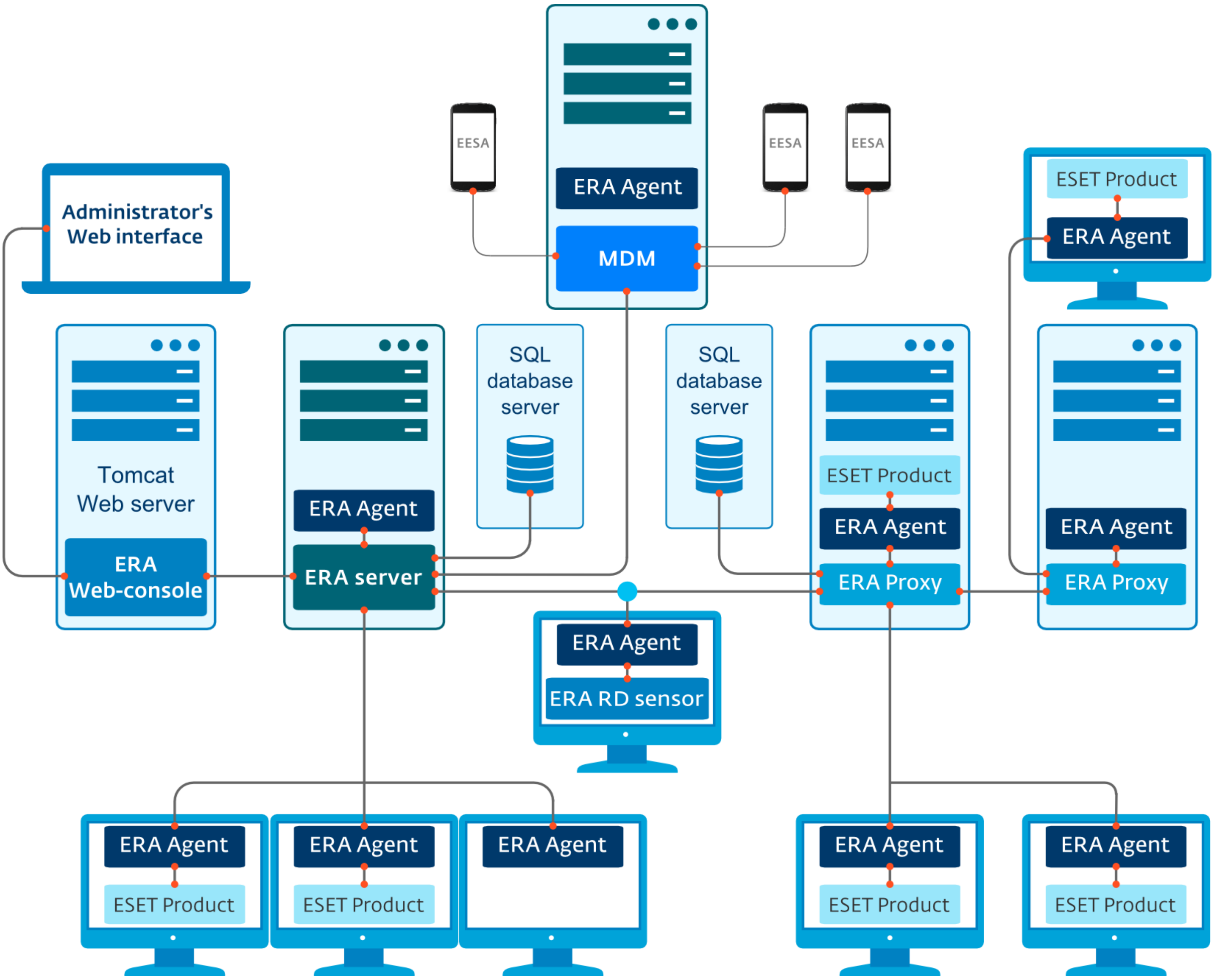
NOTE: Dual SIM and rooted devices are not supported. Some features (for example, Anti-Theft and SMS & Call Filter) are not available on tablets that do not support calling and messaging.

2. Users connecting to ESET Remote Administrator

ESET Remote Administrator (ERA) 6 is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Remote Administrator task management system allows you to install ESET security solutions on remote computers and mobile devices and quickly respond to new problems and threats. ESET Remote Administrator does not provide protection against malicious code on its own, it relies on the presence of an ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, OS X and operating systems that run on mobile devices (mobile phones and tablets).

The picture below depicts a sample architecture for a network protected by ESET security solutions managed by ERA:



NOTE: For more information see the ESET Remote Administrator online documentation.

2.1 ESET Remote Administrator Server

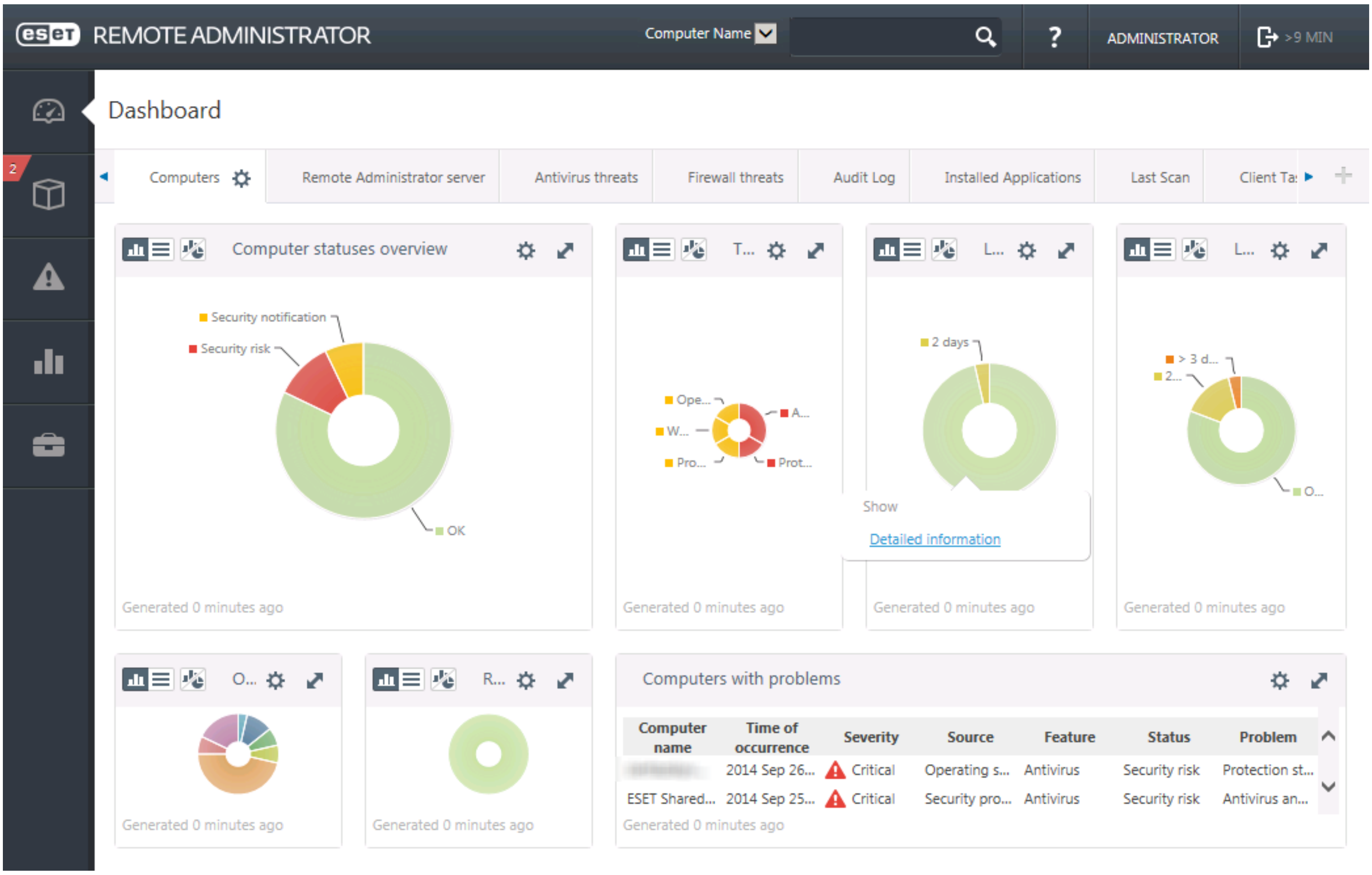
ESET Remote Administrator Server is the executive component of ESET Remote Administrator. It processes all data received from clients that connect to the Server (through the ERA Agent). The ERA Agent facilitates communication between the client and the server. Data (Client logs, configuration, agent replication, etc.) are stored in a database that ERA accesses to provide reporting.

To correctly process the data, the ERA Server requires a stable connection to a database server. We recommend that you install ERA Server and your database on separate servers to optimize performance. The machine on which ERA Server is installed must be configured to accept all Agent/Proxy/RD Sensor connections which are verified using certificates. Once ERA Server is installed, you can open ERA Web Console which allows you to manage endpoint workstations with ESET solutions installed.

2.2 Web Console

ERA Web Console is a web-based user interface that presents data from ERA Server and allows you to manage ESET security solutions in your network. Web Console can be accessed using a browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. You can choose to make the web server accessible from the internet to allow for the use of ESET Remote Administrator from virtually any place or device.

The Web Console Dashboard:



Computers with problems

Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
[redacted]	2014 Sep 26...	⚠ Critical	Operating s...	Antivirus	Security risk	Protection st...
ESET Shared...	2014 Sep 25...	⚠ Critical	Security pro...	Antivirus	Security risk	Antivirus an...

Generated 0 minutes ago

The **Quick Search** tool is located at the top of the Web Console. Select **Computer Name**, **IPv4/IPv6 Address** or **Threat Name** from the drop-down menu, type your search string into the text field, and then click the magnifier symbol or press **Enter** to search. You will be redirected to the **Groups** section, where your search result will be displayed.

2.3 Proxy

ERA Proxy is another component of ESET Remote Administrator with two main purposes. In a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies facilitating the main ERA Server. The other advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that the ERA Agent on each client is not connecting to the main ERA Server directly via ERA Proxy, which is on the same local network as the branch office. This configuration frees up the link to the branch office. The ERA Proxy accepts connections from all local ERA Agents, compiles data from them and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

Depending on your network configuration, it is possible for ERA Proxy to connect to another ERA Proxy and then connect to the main ERA Server.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

2.4 Agent

ERA Agent is an essential part of the ESET Remote Administrator product. ESET security solutions on client machines (for example ESET Endpoint Security) communicate with ERA Server through the Agent. This communication allows for the management of ESET security solutions on all remote clients from a one central location. The Agent collects information from the client and sends it to the Server. When the Server sends a task to a client, the task is sent to the Agent which then communicates with the client. All network communication happens between the Agent and the upper part of the ERA network – Server and Proxy.

The ESET Agent uses one of the following three methods to connect to the Server:

1. The Client's Agent connected directly to the Server.
2. The Client's Agent connects via a Proxy that is connected to the Server.
3. The Client's Agent connects to the Server through multiple Proxies.

The ERA Agent communicates with ESET solutions installed on a client, collects information from programs on that client and passes configuration information received from the Server to the client.

NOTE: The ESET proxy has its own Agent which handles all communication tasks between clients, other proxies and the ERA Server.

2.5 RD Sensor

RD (Rogue Detection) Sensor is a part of ESET Remote Administrator designed to find computers on your network. RD Sensor lets you easily add new computers to ESET Remote Administrator without the need to find and add them manually. Every computer found on your network is displayed in the Web Console and added to the default **All** group. From here, you can take further actions with individual client computers.

RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. The ERA Server evaluates whether the PCs found on the network are unknown or already managed.

3. Remote installation

Remote installation of ESET Endpoint Security from ERA requires the following:

- Installation of Mobile Device Connector
- Mobile devices enrollment

The installation of ESET Endpoint Security itself can be done in two ways:

1. Admin sends the Enrollment link to the end-users via email along with the installation APK file and a brief explanation on how to install it. By tapping the link, users are redirected to the default internet browser of their Android device and ESET Endpoint Security will be enrolled and connected to ERA. If ESET Endpoint Security is not installed on the device, they will be automatically redirected to the Google Play store to download the app. After that, a standard installation will follow.
2. Admin sends the application settings file to the end-users via email along with the installation APK file and a brief explanation on how to install it. Alternatively, users will be prompted to download the APK file from the Google Play store – admin provides the link. After the installation, the users open the application settings file. All the settings will be imported and the application will be activated (provided the license information was included).

4. Local installation on the device

ESET Endpoint Security provides administrators with an option to setup and manage Endpoint locally if they choose not to use ESET Remote Administrator. All application settings are protected by Admin password so the application is under full administration control at all times.

If the administrator in a small company decides not to use ESET Remote Administrator but he still wants to protect corporate devices and apply basic security policies, he has two options on how to manage the devices locally:

1. Physical access to each company device and a manual configuration of the settings.
2. Administrator can prepare desired configuration on his Android device (with ESET Endpoint Security installed) and export these settings to a file – see the Import/Export settings section of this guide for more info). Administrator can share the exported file with the end-users (for example via email) – they can import the file to any device running ESET Endpoint Security. When the user opens and accepts the received settings file, it will automatically import all the settings and activate the application (provided the license information was included). All the settings will be protected by Admin password.

4.1 Download from ESET website

Download ESET Endpoint Security by scanning the QR code below using your mobile device and a QR scanning app:

Alternatively, you can download the ESET Endpoint Security installation APK file from ESET website:

1. Download the installation file from the ESET website.
2. Open the file from the Android notification area or locate it using a file browsing manager application. The file is usually saved to the Download folder.
3. Make sure that applications from Unknown sources are allowed on your device. To do so, tap the Launcher icon ▦ on the Android home screen or go to **Home** > **Menu**. Tap **Settings** > **Security**. The **Unknown sources** option has to be allowed.
4. After opening the file, tap **Install**.

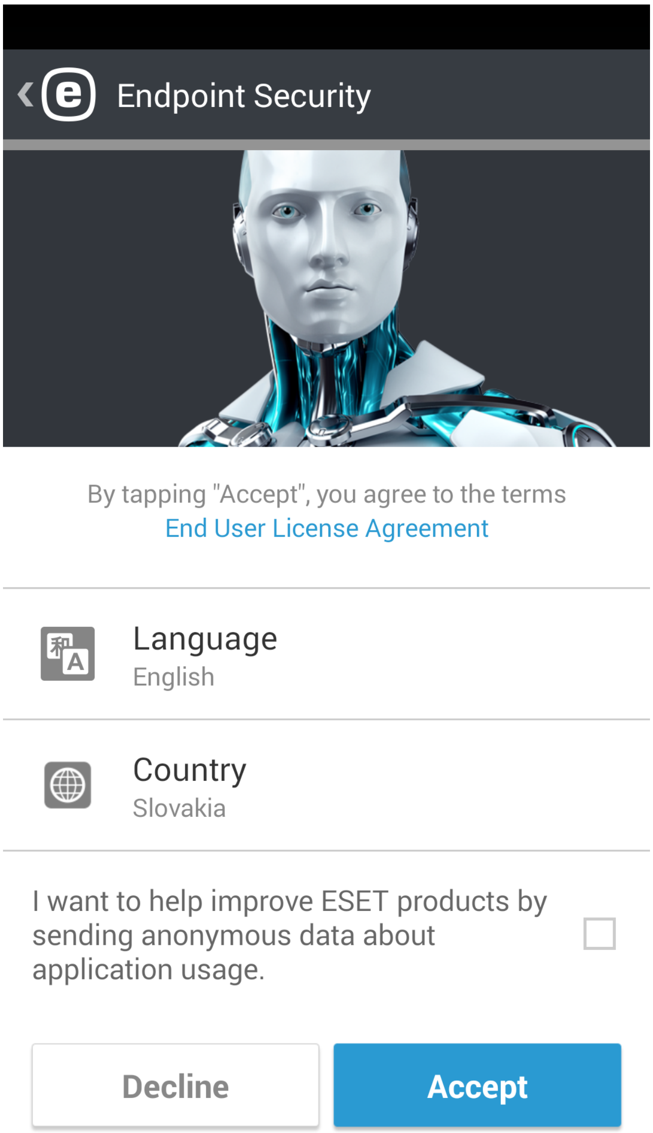
4.2 Download from Google Play

Open the Google Play Store application on your Android device and search for ESET Endpoint Security (or just ESET).

Alternatively, you can download the program by using this link or scanning the QR code below:

https://play.google.com/store/apps/details?id=com.eset.endpoint

4.3 Start-up wizard



Endpoint Security

By tapping "Accept", you agree to the terms End User License Agreement

Language
English

Country
Slovakia

I want to help improve ESET products by sending anonymous data about application usage. □

Once the application is installed, tap **Admin setup** and follow the prompts from the start-up wizard. This procedure is intended for Administrators only:

1. Select the **Language** you want to use in ESET Endpoint Security.
2. Select the **Country** you currently work or reside in.
3. If you want to help improve ESET products by sending anonymous data about application usage, select the appropriate option.
4. Tap **Accept**. By doing this, you agree to the End User License Agreement.
5. Tap **Accept** to accept the User consent.
6. Choose whether to connect ESET Endpoint Security to ESET Remote Administrator or perform a manual setup.
7. Manual setup requires product activation.
8. Create an Admin password.
9. **Uninstall protection** restricts unauthorized users from uninstalling ESET Endpoint Security. Tap **Enable** and then tap **Activate** at the **Device administrator** prompt.
10. Choose whether to participate in ESET LiveGrid. To read more about ESET LiveGrid, see this section.
11. Choose whether you want ESET Endpoint Security to detect Potentially unwanted applications. More details about such applications can be found in this section.

5. Uninstallation

ESET Endpoint Security can be uninstalled using the Uninstall wizard available from the program's main menu under **Settings** > **Uninstall**. If Uninstall protection is enabled, you will be asked to enter the Admin Password.

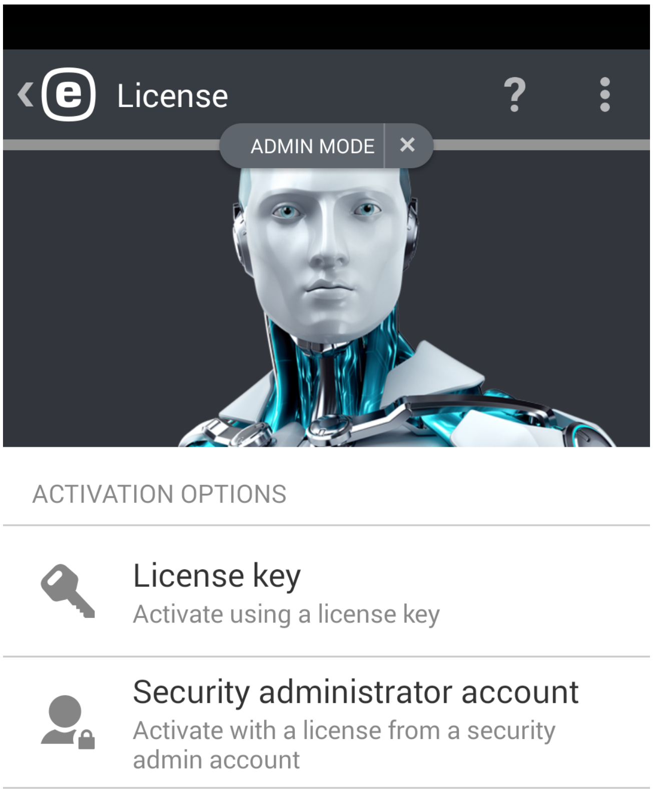
Alternatively, you can uninstall the product manually by following these steps:

1. Tap the Launcher icon ▦ on the Android home screen (or go to **Home** > **Menu**) and tap **Settings** > **Security** > **Device administrators**. Deselect **ESET Endpoint Security** and tap **Deactivate**. Tap **Unlock** and enter the Admin Password. If you have not set ESET Endpoint Security as the Device administrator, skip this step.
2. Go back to the **Settings** and tap **Manage apps** > **ESET Endpoint Security** > **Uninstall**.

6. Product activation

There are multiple ways to activate ESET Endpoint Security. The availability of a particular activation method may vary depending on the country, as well as the means of distribution (ESET web page, etc.) for your product.

To activate ESET Endpoint Security directly on the Android device, tap the **Menu** icon ⋮ in the ESET Endpoint Security main screen (or press the **MENU** button on your device) and tap **License**.


License
?
ADMIN MODE
ACTIVATION OPTIONS
License key
Activate using a license key
Security administrator account
Activate with a license from a security admin account

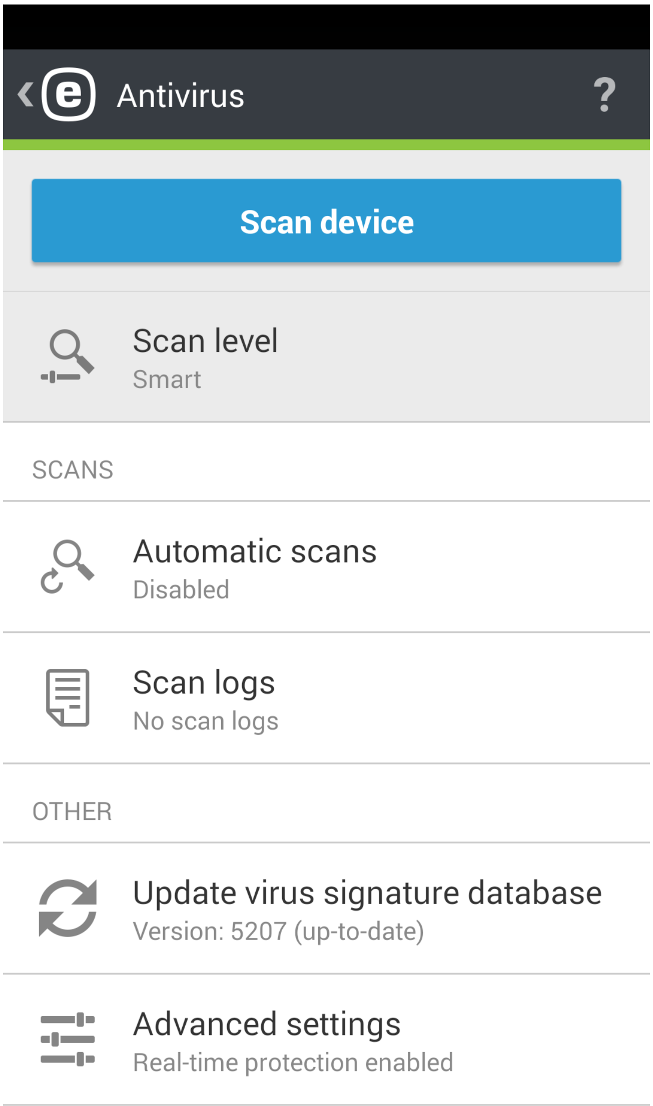
You can use any of the following methods to activate ESET Endpoint Security:

- **License key**—A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and activation of the license.
- **Security administrator account**—An account created on the ESET License Administrator portal with credentials (email address and password). This method allows you to manage multiple licenses from one location.

NOTE: ESET Remote Administrator is able to activate client devices silently using licenses made available by the administrator.

7. Antivirus

The Antivirus module safeguards your device against malicious code by blocking threats and then cleaning or quarantining them.



Scan level
Smart

SCANS

Automatic scans
Disabled

Scan logs
No scan logs

OTHER

Update virus signature database
Version: 5207 (up-to-date)

Advanced settings
Real-time protection enabled

Scan Device

Scan Device can be used to check your device for infiltrations.

Certain predefined file types are scanned by default. A complete device scan checks the memory, running processes and their dependent dynamic link libraries as well as files that are part of internal and removable storage. A brief summary of the scan will be saved to a log file available in the Scan Logs section.

If you want to abort a scan already in progress, tap the ☒ icon.

Scan Level

There are 2 different scan levels to choose from:

- **Smart** — Smart Scan will scan installed applications, DEX files (executable files for Android OS), SO files (libraries) and ZIP files with a maximum scanning depth of 3 nested archives and SD card content.
- **In-depth** — all file types regardless of their extension will be scanned both in internal memory and SD card.

Automatic Scans

In addition to On-demand device scan, ESET Endpoint Security also offers automatic scans. To learn how to use On-Charger Scan and Scheduled Scan, read this section.

Scan Logs

The Scan Logs section contains comprehensive data about completed scans in the form of log files. See the Antivirus Scan Logs section of this document for more information.

Update virus signature database

By default, ESET Endpoint Security includes an update task to ensure that the program is updated regularly. To run the update manually, tap **Update virus signature database**.

NOTE: To prevent unnecessary bandwidth usage, updates are issued as needed when a new threat is added. While updates are free with your active license, you may be charged by your mobile service provider for data transfers.

Detailed descriptions of the Antivirus Advanced settings can be found in the Advanced settings section of this document.

7.1 Automatic Scans

Scan Level

There are 2 different scan levels to choose from. This setting will apply to both On-Charger Scan and Scheduled Scan:

- **Smart** — Smart Scan will scan installed applications, DEX files (executable files for Android OS), SO files (libraries) and ZIP files with a maximum scanning depth of 3 nested archives and SD card content.
- **In-depth** — all file types regardless of their extension will be scanned both in internal memory and SD card.

On-Charger Scan

When this is selected, the scan will start automatically when the device is in an idle state (fully charged and connected to a charger).

Scheduled Scan

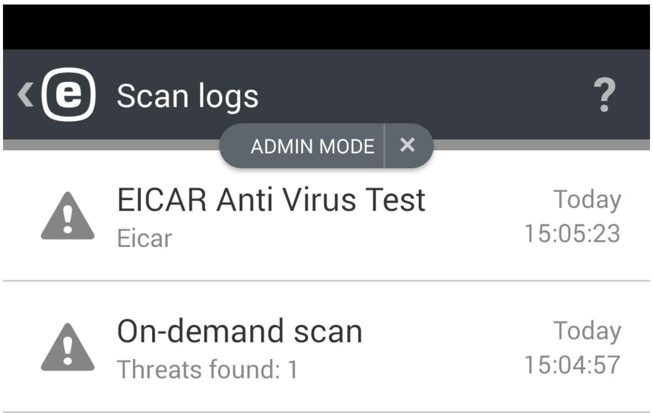
Scheduled Scan allows you to run a Device scan automatically at a predefined time. To schedule a scan, tap ○ next to **Scheduled Scan** and specify the dates and times for the scan to be launched. By default, Monday 4 am is selected.

7.2 Scan Logs

Scan Logs are created after each Scheduled scan or manually triggered Device scan.

Each log contains:

- date and time of the event
- duration of the scan
- number of scanned files
- scan result or errors encountered during the scan



EICAR Anti Virus Test
Eicar
Today
15:05:23

On-demand scan
Threats found: 1
Today
15:04:57

7.3 Ignore rules

If you manage ESET Endpoint Security remotely from ERA, you have the option to define files that will not be reported as malicious. Files added to **Ignore rules** will be ignored in future scans. To create a rule, you must specify the following:

- a file name with a proper "apk" extension
- an application package name, e.g. *uk.co.extorian.EICARAntiVirusTest*
- the name of the threat as detected by antivirus programs, e.g. *Android/MobileTX.A* (this field is mandatory)

NOTE: This feature is not available in the ESET Endpoint Security app.

7.4 Advanced settings

Real-time protection

This option allows you to enable/disable the Real-time scanner. This scanner launches automatically at system startup and scans files that you interact with. It automatically scans the Download folder, APK installation files and all files on the SD card after it is mounted.

ESET LiveGrid

Built on the ThreatSense.Net advanced early warning system, ESET LiveGrid is designed to provide additional levels of security to your device. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. Additionally, your scans are processed faster and more precisely as the ESET LiveGrid database grows over time. This allows us to offer better proactive protection and scanning speed to all ESET users. We recommend that you activate this feature. Thank you for your support.

Detect potentially unwanted applications

An unwanted application is a program that contains adware, installs toolbars, traces your search results or has other unclear objectives. There are some situations where you may feel that the benefits of the unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software.

Detect potentially unsafe applications

There are many legitimate applications whose function is to simplify the administration of networked devices. However, in the wrong hands, they may be misused for malicious purposes. The Detect Potentially Unsafe Applications option allows you to monitor these types of applications and block them if you prefer. *Potentially unsafe applications* is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications and keyloggers.

Block unresolved threats

This setting determines the action that will be performed after the scan is complete and threats are found. If you enable this option, ESET Endpoint Security will block access to files categorized as threats.

Virus signature database updates

This option allows you to set the time interval on which threat database updates are automatically downloaded. These updates are issued as needed when a new threat is added to the database. We recommend that you leave this set to the default value (daily).

Custom max database age

This setting defines the length of time between virus signature database updates after which you will be notified to update ESET Endpoint Security.

Update server

Using this option, you can choose to update your device from the **Pre-release server**. Pre-release updates have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times. The list of current modules can be found in the **About** section: tap the Menu icon ⋮ in the ESET Endpoint Security main screen and tap **About** > **ESET Endpoint Security**. It is recommended that basic users leave the **Release server** option selected by default.

ESET Endpoint Security allows you to create copies of update files that can be used to update other devices on the network. The use of a **Local mirror** – a copy of the update files in the LAN environment – is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each mobile device. Detailed information on how to configure the mirror server using ESET Endpoint products for Windows can be found in this document.

8. Anti-Theft

The **Anti-Theft** feature protects your mobile device from unauthorized access.

If you lose your device or someone steals it and replaces your SIM card with a new (untrusted) one, the device will automatically be locked by ESET Endpoint Security and an alert SMS will be sent to user-defined phone number(s). This message will include the phone number of the currently inserted SIM card, the IMSI (International Mobile Subscriber Identity) number and the phone's IMEI (International Mobile Equipment Identity) number. The unauthorized user will not be aware that this message has been sent because it will automatically be deleted from your device's messaging threads. You can also request the GPS coordinates of your lost mobile device, or remotely erase all data stored on the device.

NOTE: Certain Anti-Theft features (Trusted SIM cards and SMS Text Commands) are not available on tablets that do not support messaging.

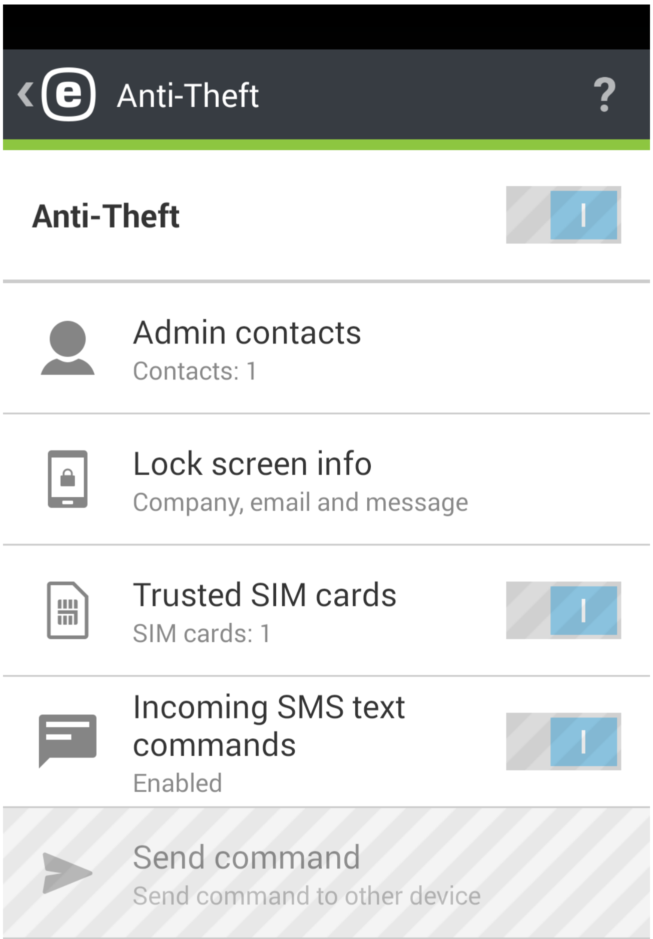
Anti-Theft features help administrators protect and locate a missing device. Actions may be triggered either from ERA or via SMS commands.

ESET Endpoint Security 2 uses the same SMS commands from version 1 (Lock, Wipe and Find). The following entirely new commands have been added:

- **Unlock**—unlocks the locked device
- **Enhanced Factory reset**—all accessible data on the device will be quickly removed (file headers will be destroyed) and the device will be reset to its default factory settings
- **Siren**—the lost device will be locked and it will play a very loud sound even if the device is set to mute

To strengthen the security of SMS commands, the administrator will receive a unique and time-limited verification SMS code on his mobile phone (at the number defined in the Admin contacts list) when he executes an SMS command. This verification code will be used to verify a particular command.

For example, if an administrator sends an SMS to a managed device (for example, a lost mobile phone) with the text *eset lock,* they will receive an SMS with a verification code for that command. The administrator then sends a new SMS to the same phone number with the text *eset lock* followed by the confirmation code. After these steps, the command will be verified and executed. SMS commands can be sent from any mobile phone and any mobile number listed in the Admin contacts.



Anti-Theft

Anti-Theft

Admin contacts
Contacts: 1

Lock screen info
Company, email and message

Trusted SIM cards
SIM cards: 1

Incoming SMS text commands
Enabled

Send command
Send command to other device

When executing commands via SMS, the administrator receives a confirmation SMS that a particular command was sent. When executing commands from ERA, the administrator receives a confirmation in ERA.

When receiving location info (**Find** command), the administrator using ESET Remote Administrator receives the location information in the form of GPS coordinates. When executing the command via SMS, the location information (GPS coordinates and a link to Google Maps) is received via SMS. When using the GUI for SMS commands (the **Send command** feature), the received information is presented in the dedicated GUI.

All Anti-Theft commands can be performed from ERA as well. New mobile device management functionality allows the administrators to perform the Anti-Theft commands just by few clicks. Tasks are immediately submitted for executions via a new push-commands processing component (Mobile Device Connector) that is now a part of ERA infrastructure.

8.1 Administrator contacts

This is the List of administrator phone numbers protected by the admin password. Anti-Theft commands can only be sent from trusted numbers. These numbers are also used for notifications related to Anti-Theft actions.

8.1.1 How to add administrator contact

A name of the administrator and the phone number is supposed to be entered during the Anti-Theft start-up wizard. If the contact contains more than one phone number, all associated numbers will be taken into account.

Admin contacts can be added or modified in the **Anti-Theft** > **Admin contacts** section.

8.2 Lock screen info

The administrator is able to define custom information (company name, email address, message) which will be displayed when the device is locked, with the option to call one of the pre-defined admin contacts.

This information includes:

- Company name (optional)
- Email address (optional)
- A custom message

8.3 Trusted SIM cards

The **Trusted SIM** section shows the list of trusted SIM cards that will be accepted by ESET Endpoint Security. If you insert a SIM card not defined in this list, the screen will be locked and an alert SMS will be sent to the administrator.

To add a new SIM card, tap the ✚ icon. Enter a **Name** for the SIM card (for example, Home, Work) and its IMSI (International Mobile Subscriber Identity) number. IMSI is usually presented as a 15-digit long number printed on your SIM card. In some instances, it may be shorter.

To remove a SIM card from the list, touch and hold the entry, and then tap the 🗑 icon.

NOTE: The Trusted SIM feature is not available on CDMA, WCDMA and WiFi-only devices.

8.4 Remote commands

Remote commands can be triggered three ways:

- directly from ERA Console
- using the **Send command** feature in ESET Endpoint Security installed on the admin's Android device
- by sending SMS text messages from admin's device

To make the execution of the SMS commands easier for an administrator not using ERA, commands can be triggered from ESET Endpoint Security installed on the admin's Android device. Instead of manually typing the text message and verifying the command with the verification code, the admin can use the **Send command** feature (only available in Admin mode). An administrator can enter the phone number or choose a contact and select the command to send from the drop-down menu. ESET Endpoint Security will automatically execute all necessary steps silently in the background.

When sending SMS commands, an admin's phone number must be an Administrator contact on the target device. The administrator will receive a verification code valid for one hour that can be used to execute any of the commands listed below. The code should be appended to the message where the command is sent in the following format: `eset find code`. The administrator will receive a confirmation once the command has been executed on the target device. The following SMS commands can be sent:

Find
SMS command: `eset find`
You will receive a text message with the GPS coordinates of the target device, including a link to its location on Google maps. The device will send a new SMS if a more precise location is available after 10 minutes.

Lock
SMS command: `eset lock`
This will lock the device—you will be able to unlock it using the Admin password or the Unlock remote command. When sending this command via SMS, you can append a custom message that will be displayed on the locked device's screen. Use the following format: `eset lock code message`. If you leave the message parameter empty, a message from the Lock screen info section will be displayed.

Unlock
SMS command: `eset unlock`
The device will be unlocked and the SIM card currently in the device will be saved as a Trusted SIM.

Siren
SMS command: `eset siren`
A loud siren will play even if the device is set to mute.

Enhanced factory reset
SMS command: `eset enhanced factory reset`
This will reset the device to its factory settings. All accessible data will be erased and file headers will be removed. The process can take several minutes.

Wipe
SMS command: `eset wipe`
All contacts, messages, emails, accounts, SD card content, pictures, music and videos stored in default folders will be permanently erased from your device. ESET Endpoint Security will remain installed.

NOTE: SMS commands are not case sensitive.

9. Application Control

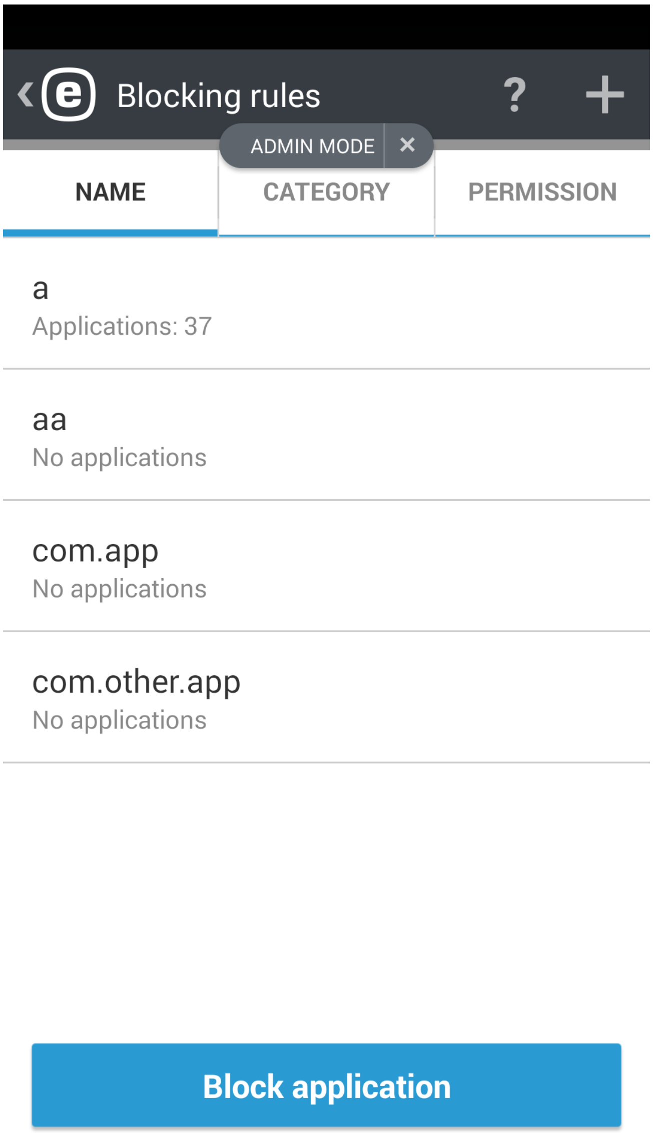
The **Application Control** feature offers administrators the option to monitor installed applications, block access to defined applications, and lower the risk of exposure by prompting the users to uninstall certain applications. The administrator can select from several filtering methods for applications:

- Manually define applications that should be blocked
- Category-based blocking (for example, games or social)
- Permission-based blocking (for example, applications that track location)
- Blocking by source (for example, applications installed from sources other than the Google Play store)

9.1 Blocking Rules

In the **Application Control** > **Blocking** > **Blocking rules** section, you can create the application blocking rules based on the following criteria:

- application name or package name
- category
- permissions



a
Applications: 37

aa
No applications

com.app
No applications

com.other.app
No applications

9.1.1 Blocking by application name

ESET Endpoint Security gives administrators the option to block an application according to its name or the package name. The **Blocking rules** section provides an overview of the created rules and the list of blocked applications.

To modify an existing rule, touch and hold the rule and then tap **Edit** ✎ . To remove rule entries from the list, touch and hold one of the entries, select the ones you want to remove and then tap **Remove** 🗑 . To clear the entire list, tap **SELECT ALL** and then tap **Remove** 🗑.

When you block an application by name, ESET Endpoint Security will look for the exact match with a name of launched application. If you change the ESET Endpoint Security GUI to a different language, you must reenter the application name in that language to continue blocking it.

In order to avoid any issues with localized application names, we recommend that you block such applications by their package names – a unique application identifier that cannot be changed during runtime or reused by another application.

In the case of a local administrator, a user can find the application package name in **Application Control** > **Monitoring** > **Allowed applications**. After tapping the application, the **Detail** screen will display the application package name. To block the application, follow these steps.

9.1.1.1 How to block an application by its name

1. Tap **Application Control** > **Blocking** > **Block application** > **Block by name**.
2. Choose whether to block the application according to its name or the name of the package.
3. Enter the words based on which the application will be blocked. To divide multiple words, use a comma (,) as a delimiter.

For example, a word "*poker*" in the **Application name** field will block all applications containing "*poker*" in its name. If you enter "*com.poker.game*" into the **Package name** field, ESET Endpoint Security will block just one application.

9.1.2 Blocking by application category

ESET Endpoint Security gives admin the option to block the application according to pre-defined application categories. The **Blocking rules** section provides you with an overview of the created rules and the list of blocked applications.

If you want to modify the existing rule, touch and hold the rule and tap **Edit** ✎ .

To remove some rule entries from the list, touch and hold one of the entries, select the ones you want to remove and tap **Remove** 🗑 . To clear the entire list, tap **SELECT ALL**.

9.1.2.1 How to block an application based on its category

1. Tap **Application Control** > **Blocking** > **Block application** > **Block by category**.
2. Select the pre-defined categories using check-boxes and tap **Block**.

9.1.3 Blocking by application permissions

ESET Endpoint Security gives admin the option to block the application according to its permissions. The **Blocking rules** section provides you with an overview of the created rules and the list of blocked applications.

If you want to modify the existing rule, touch and hold the rule and tap **Edit** ✎ .

To remove some rule entries from the list, touch and hold one of the entries, select the ones you want to remove and tap **Remove** 🗑 . To clear the entire list, tap **SELECT ALL**.

9.1.3.1 How to block an application by its permissions

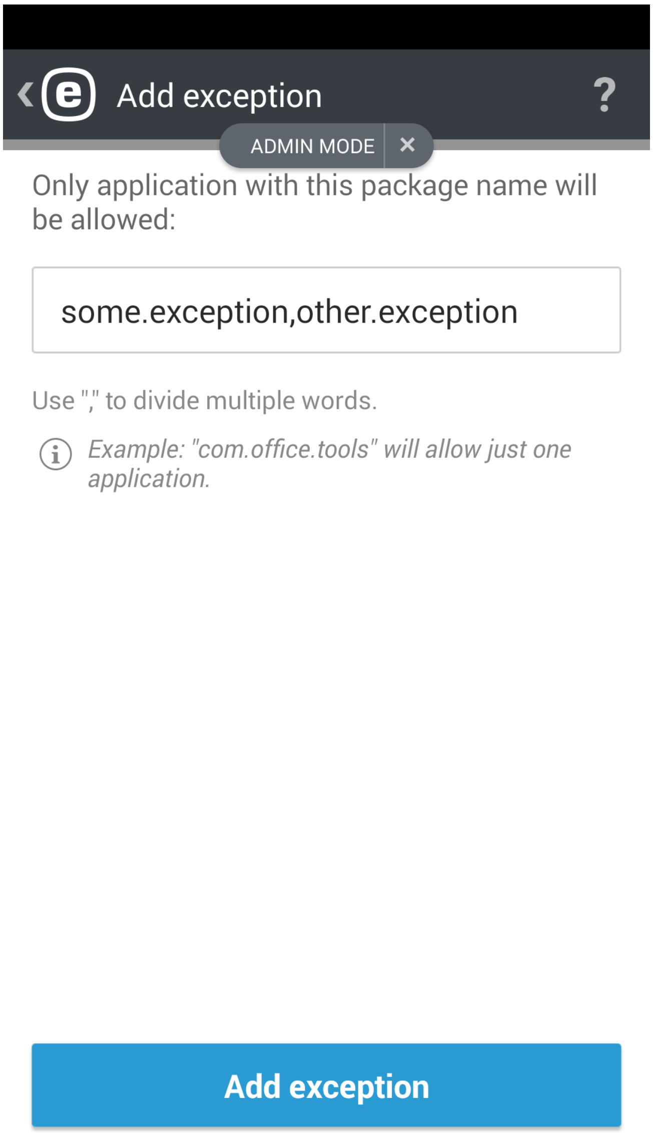
1. Tap **Application Control** > **Blocking** > **Block application** > **Block by permission**.
2. Select the permissions using check-boxes and tap **Block**.

9.1.4 Block unknown sources

By default, ESET Endpoint Security does not block the applications obtained from the internet or any source other than the Google Play store. The **Blocked applications** section provides you with an overview of blocked applications (package name, rule applied) and the option to uninstall the application or add it to the whitelist – **Exceptions** section.

9.2 Exceptions

You can create exceptions to exclude a specific application from the list of blocked applications. Administrators managing ESET Endpoint Security remotely can use this new feature to determine whether a particular device is in compliance with the company policy regarding installed applications.



Only application with this package name will be allowed:

some.exception,other.exception

Use "," to divide multiple words.

Example: "com.office.tools" will allow just one application.

9.2.1 How to add exceptions

Apart from adding the new exception (entering the application package name), applications can be also whitelisted by exempting them from the list of **Blocked applications**.

9.3 Required applications

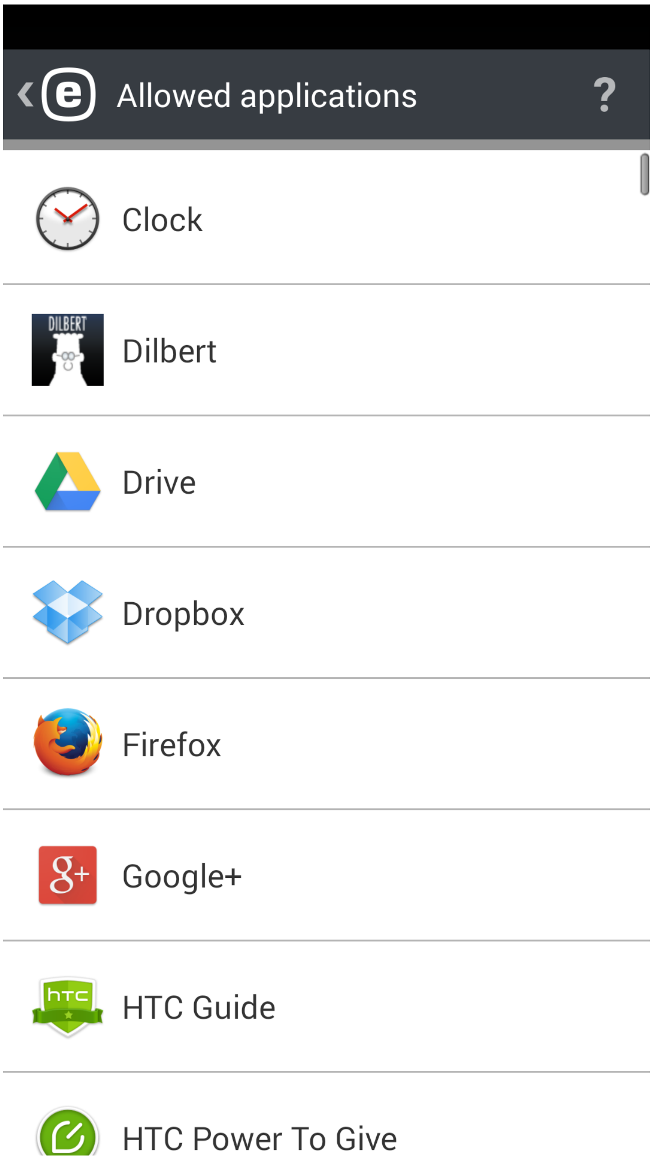
If you manage ESET Endpoint Security remotely from ERA, you have the option to define which applications must be installed on the target device(s). The following information is required:

- name of the application visible to the user
- unique application package name, e.g. *com.eset.ems2.gp*
- URL where a user can find a download link. You can also use Google Play links, e.g. *https://play.google.com/store/apps/details?id=com.eset.ems2.gp*

NOTE: This feature is not available in the ESET Endpoint Security app.

9.4 Allowed applications

This section provides you with an overview of installed applications that are not blocked by blocking rules.



Allowed applications

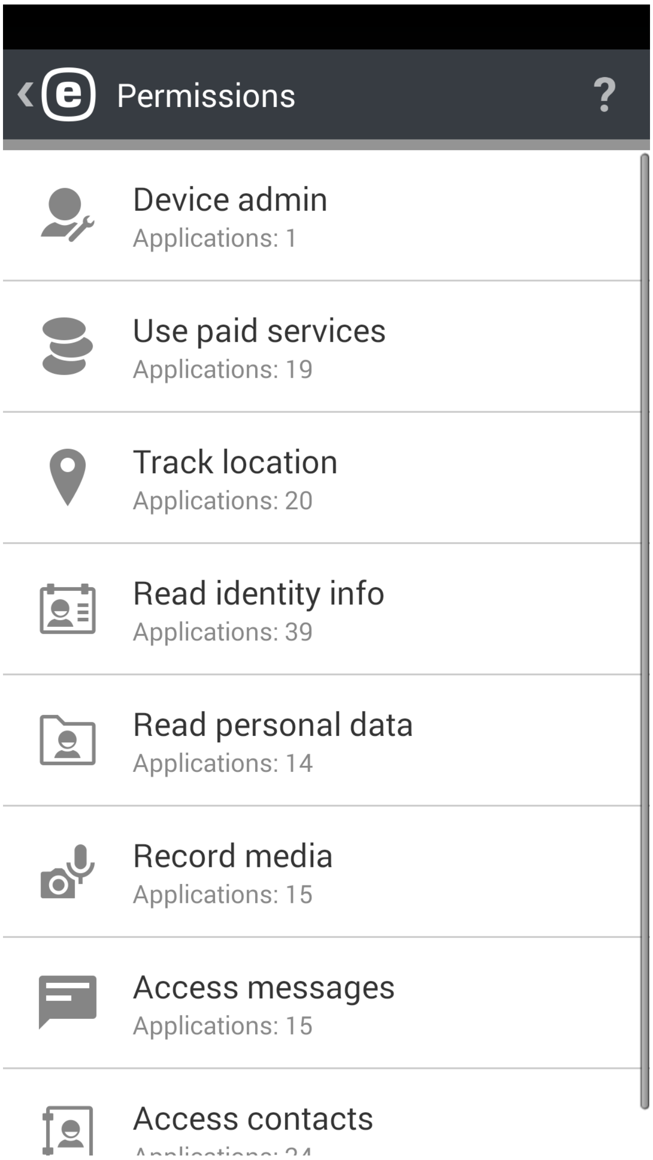
- Clock
- Dilbert
- Drive
- Dropbox
- Firefox
- Google+
- HTC Guide
- HTC Power To Give

9.5 Permissions

This feature tracks the behavior of applications with access to personal or company data, and allows the administrator to monitor application access based on pre-defined permissions categories.

Some applications installed on your device might have access to services that cost you money, track your location or read your identity info, contacts or text messages. ESET Endpoint Security provides an audit of these applications.

In this section, you can see the list of applications sorted by categories. Tap each category to see its detailed description. Permissions details of each application can be accessed by tapping a particular application.



Device admin
Applications: 1

Use paid services
Applications: 19

Track location
Applications: 20

Read identity info
Applications: 39

Read personal data
Applications: 14

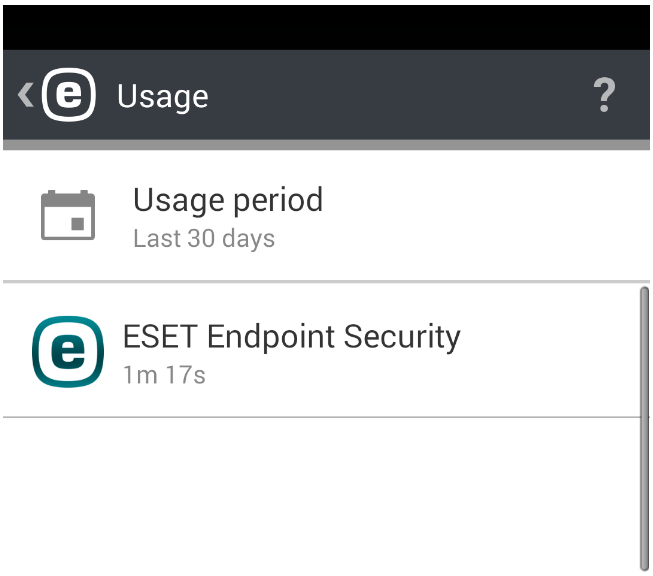
Record media
Applications: 15

Access messages
Applications: 15

Access contacts

9.6 Usage

In this section, the administrator can monitor the amount of time a user spends using specific applications. To filter the overview by its usage period, use the **Interval** option.



Usage period
Last 30 days

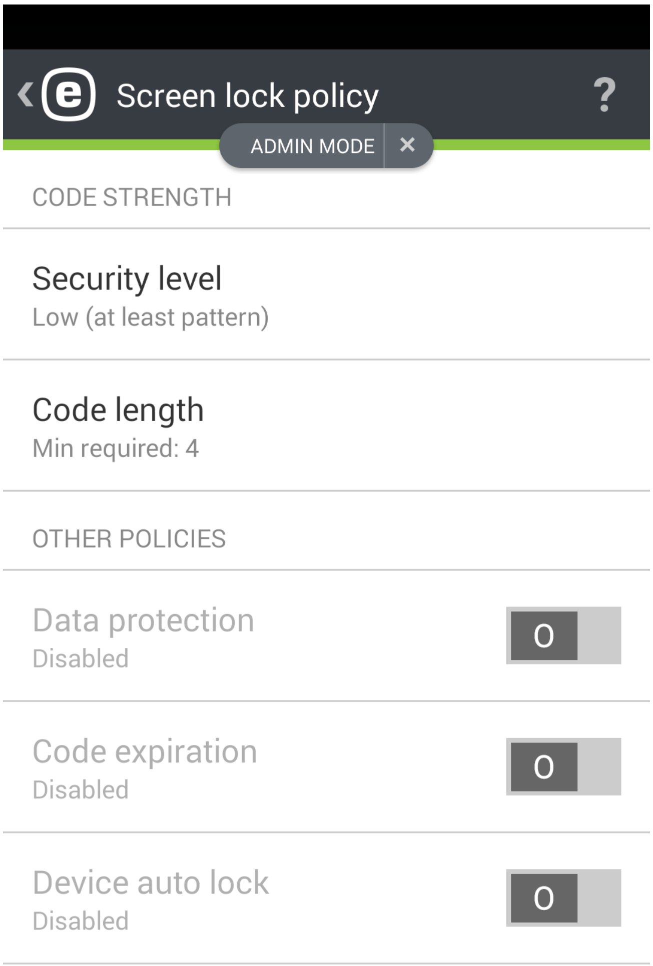
ESET Endpoint Security
1m 17s

10. Device Security

Device security provides administrators with options to perform the following:

- execute basic security policies across mobile devices and define policies for important device settings
- specify the required screen lock strength
- restrict built-in camera usage

10.1 Screen lock policy



Screen lock policy

ADMIN MODE ✕

CODE STRENGTH

Security level
Low (at least pattern)

Code length
Min required: 4

OTHER POLICIES

Data protection
Disabled

Code expiration
Disabled

Device auto lock
Disabled

In this section, the administrator is able to:

- set a minimum security level (pattern, PIN, password) for the system screen lock code, and define the complexity of the code (for example, minimum code length)
- set the maximum number of failed unlock attempts (or the device will go to factory defaults)
- set maximum screen lock code age
- set the lock screen timer

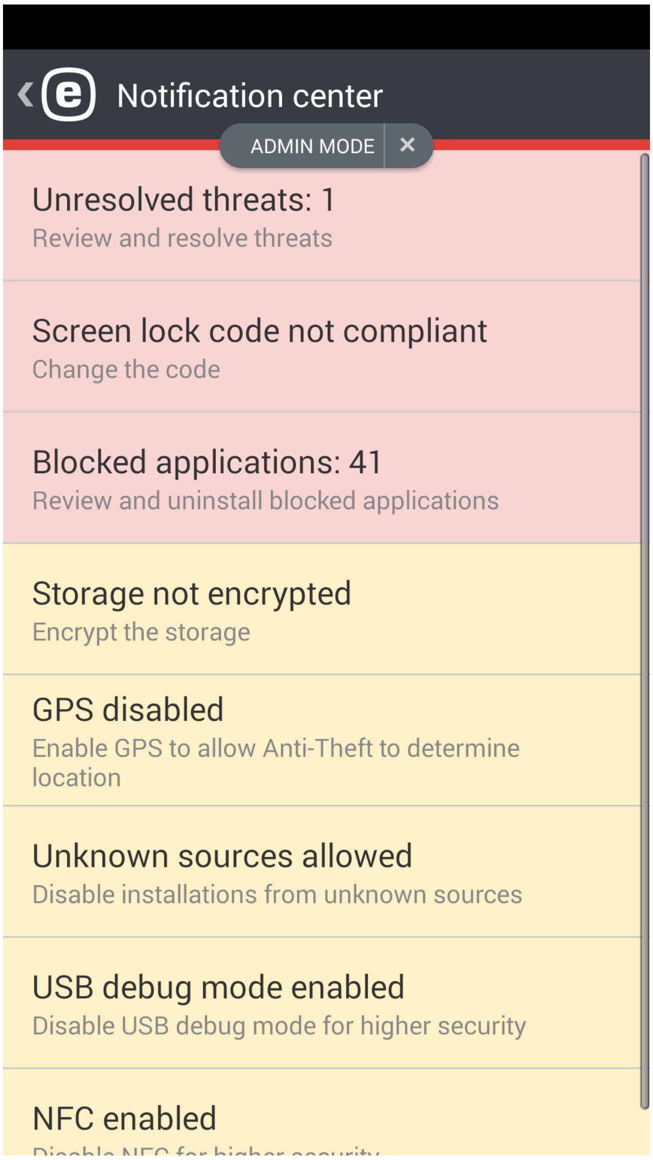
ESET Endpoint Security automatically notifies the user and the administrator if the current device settings are in compliance with corporate security policies. If a device is out of compliance, the application will automatically suggest to the user what should be changed to be compliant again.

10.2 Device settings policy

Device Security also includes your **Device Settings Policy** (previously a part of the **Security audit** functionality) which gives the system administrator the option to monitor pre-defined device settings to determine if they are in the recommended state.

Device settings include:

- Wi-Fi
- GPS satellites
- Location services
- Memory
- Data roaming
- Call roaming
- Unknown sources
- Debug mode
- NFC
- Storage encryption
- Rooted device



Unresolved threats: 1
Review and resolve threats

Screen lock code not compliant
Change the code

Blocked applications: 41
Review and uninstall blocked applications

Storage not encrypted
Encrypt the storage

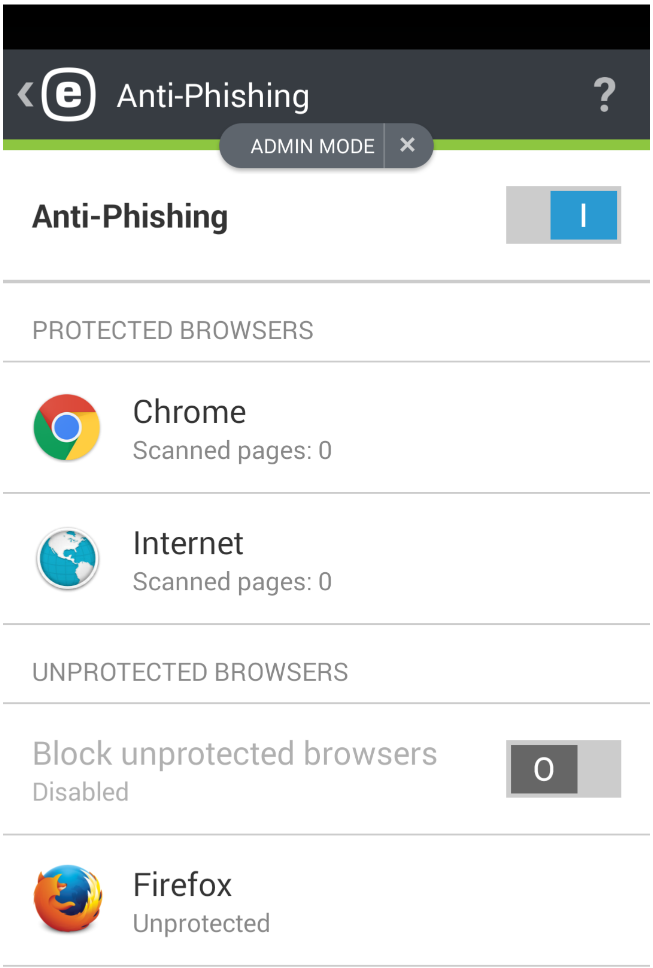
GPS disabled
Enable GPS to allow Anti-Theft to determine location

Unknown sources allowed
Disable installations from unknown sources

USB debug mode enabled
Disable USB debug mode for higher security

NFC enabled
Disable NFC for higher security

11. Anti-Phishing



Anti-Phishing

ADMIN MODE ✕

Anti-Phishing I

PROTECTED BROWSERS

Chrome
Scanned pages: 0

Internet
Scanned pages: 0

UNPROTECTED BROWSERS

Block unprotected browsers
Disabled O

Firefox
Unprotected

The term *phishing* defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames and passwords.

We recommend that you keep **Anti-Phishing** enabled. ESET Endpoint Security scans the URL addresses – all potential phishing attacks coming from websites or domains listed in the ESET malware database will be blocked and a warning notification will be displayed informing you of the attack.

IMPORTANT: Anti-Phishing integrates with the most common web browsers available on Android OS. In general, Anti-Phishing protection is available for Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung and stock browsers that come as pre-installed on Android devices. Other browsers will be listed as unprotected and the access to them can be blocked by switching the ○ button.

For the proper functioning of ESET Anti-Phishing, it is required to enable **Accessibility** in Android system settings.

12. SMS & Call Filter

SMS & Call Filter blocks incoming SMS/MMS messages and incoming/outgoing calls based on user-defined rules.

Unsolicited messages usually include advertisements from mobile phone service providers or messages from unknown or unspecified users. The term **block message** refers to moving an incoming message to the **History** section automatically. No notification is displayed when an incoming message or call is blocked. The advantage of this is that you will not be bothered by unsolicited information, but can always check the logs for messages that may have been blocked by mistake.

NOTE: SMS & Call Filter does not work on tablets that do not support calling and messaging. SMS/MMS Filtering is not available on Android OS 4.4 and later versions, and will be disabled on devices where Google Hangouts is set as the primary application for SMS.

To block calls and messages from the last received phone number, tap **Block Last Caller** or **Block Last SMS Sender**. This will create a new rule.

12.1 Rules

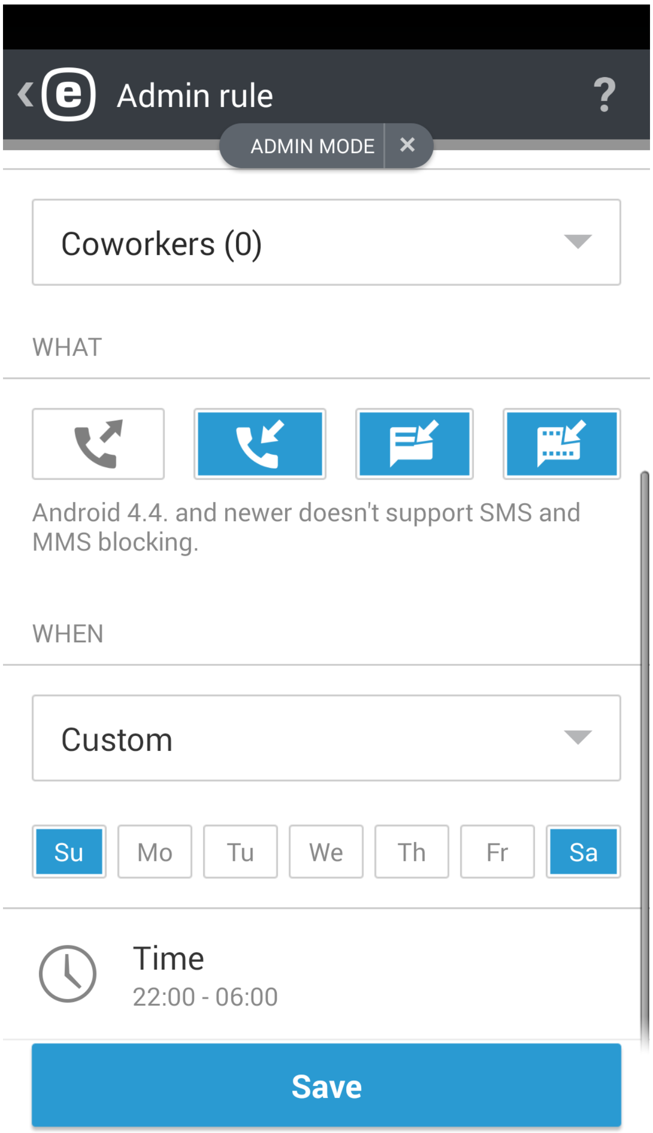
As a user, you can create user rules without a need of entering Admin password. Admin rules can be created only in Admin mode. Admin rules will overwrite any user rules.

More information about creating a new rule can be found in this section.

If you want to remove an existing rule entry from the **Rules** list, tap and hold the entry and then tap the **Remove** icon 🗑.

12.1.1 How to add a new rule

To add a new rule, tap the ✚ icon in the top right corner of the **Rules** screen.



Coworkers (0)

Android 4.4. and newer doesn't support SMS and MMS blocking.

Custom

Time
22:00 - 06:00

Based on the action you want the rule to perform, choose whether the messages and calls will be allowed or blocked.

Specify a person or a group of phone numbers. ESET Endpoint Security will recognize the contact groups saved in your Contacts (for example, Family, Friends or Coworkers). **All unknown numbers** will include the phone numbers not saved in your contact list. You can use this option to block unwelcome phone calls (for example, "cold calls") or to prevent employees from dialing unknown numbers. The **All known numbers** option refers to all phone numbers saved in your contact list. **Hidden numbers** will apply to callers that have their phone number intentionally hidden via the Calling Line Identification Restriction (CLIR).

Specify which should be blocked or allowed:

- ☎ outgoing calls
- ☎ incoming calls
- ✉ incoming text messages (SMS) or
- ✉ incoming multimedia messages (MMS)

To apply the rule for a specified time only, tap **Always** > **Custom** and select the days of the week and a time interval for which you want to apply the rule. By default, Saturday and Sunday are selected. This functionality might come in handy if you do not want to be disturbed during meetings, business trips, night or during the weekend.

NOTE: If you are abroad, all phone numbers entered in the list must include the international dialing code followed by the actual number (for example, +1610100100).

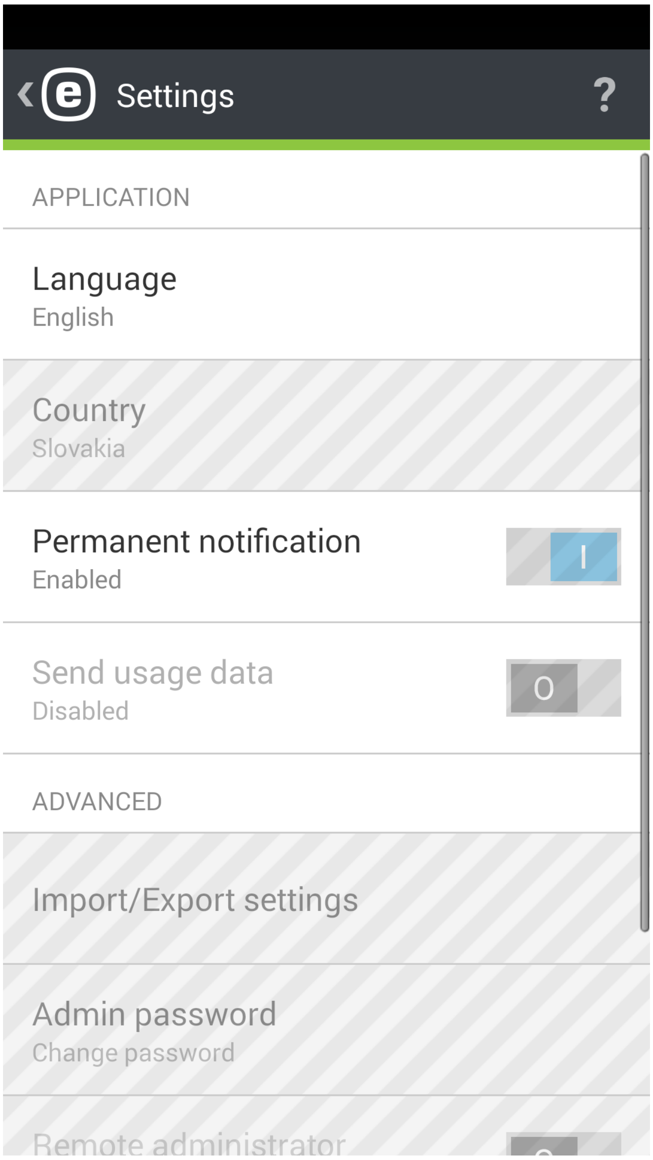
12.2 History

In the **History** section, you can see the calls and messages blocked or allowed by the SMS & Call Filter. Each log contains the name of the event, corresponding phone number, date and time of the event. SMS and MMS message logs also contain the message body.

If you want to modify a rule related to the phone number or a contact that was blocked, select the entry from the list by tapping it and tap the ✎ icon.

To remove the entry from the list, select it and tap the 🗑 icon. To remove more entries, touch and hold one of the entries, select the ones you want to remove and tap the 🗑 icon.

13. Settings



Settings

APPLICATION

Language
English

Country
Slovakia

Permanent notification
Enabled

Send usage data
Disabled

ADVANCED

Import/Export settings

Admin password
Change password

Remote administrator

Language

By default, ESET Endpoint Security is installed in the language which is set on your device as a system locale (in Android OS Language and keyboard settings). To change the language of the application user interface, tap **Language** and select the language of your choice.

Country

Select the country you currently work or reside in.

Update

For maximum protection, it is important to use the latest version of ESET Endpoint Security. Tap **Update** to see if there is a newer version available for download from ESET website. This option is not available if you downloaded ESET Endpoint Security from Google Play – in this case, the product is updated from Google Play.

Permanent notification

ESET Endpoint Security displays its notification icon ⓔ in the top left corner of the screen (Android status bar). If you do not want this icon to be displayed, deselect **Permanent notification**.

Permission notifications

See the Permission management section.

Send usage data

This option helps improve ESET products by sending anonymous data about the application usage. Sensitive information will not be sent. If you did not enable this option during the installation start-up wizard, you can do so in the **Settings** section.

Admin Password

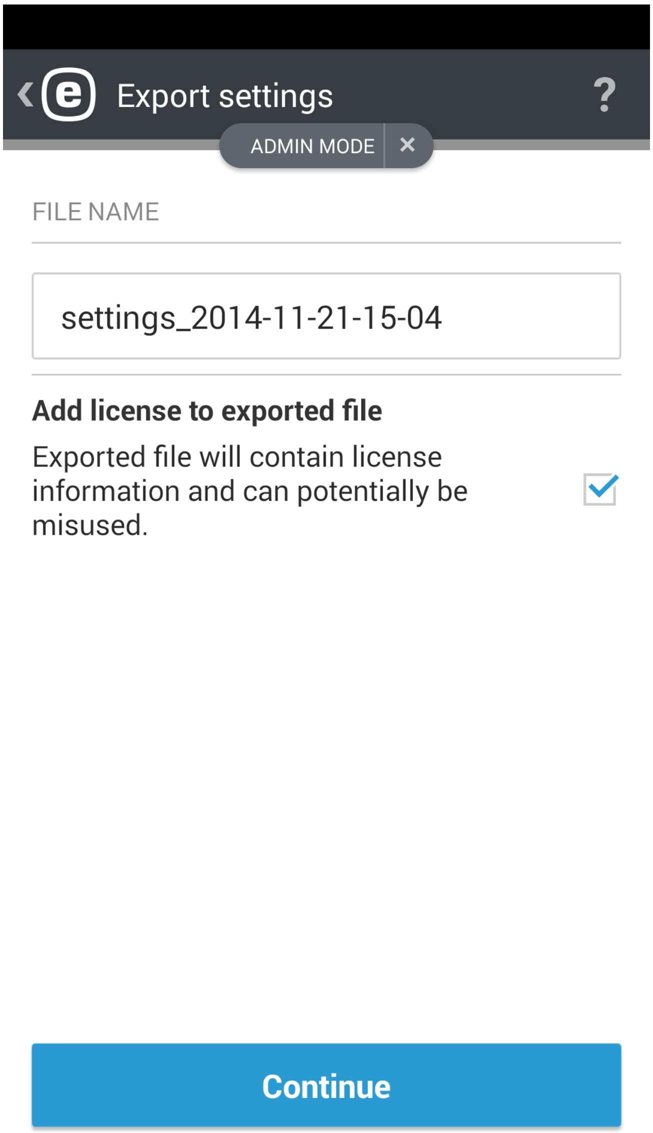
This option allows you to set a new Admin password or change the existing one. To read more, see the Admin Password section of this document.

Uninstall

By running the Uninstall wizard, ESET Endpoint Security and quarantine folders will be permanently removed from the device. If Uninstall protection was enabled, you will be asked to enter your **Admin Password**.

13.1 Import/Export settings

To easily share settings from one mobile device with another if the devices are not managed by ERA, ESET Endpoint Security 2 introduces the option to export and import program settings. The administrator can manually export device settings to a file which can then be shared (for example, via email) and imported to any device running the client application. When the user accepts the received settings file, it automatically defines all settings and activates the application (provided the license information was included). All settings will be protected by the administrator password.



FILE NAME

settings_2014-11-21-15-04

Add license to exported file

Exported file will contain license information and can potentially be misused. ☑

13.1.1 Export settings

To export the current settings of ESET Endpoint Security, specify the settings file name – the current date and time will be automatically filled in. You can also add the license information (License key or Security admin account email address and password) to the exported file but beware that this information will not be encrypted and can be misused.

In the next step, select the way you want to share the file through:

- Wi-Fi network
- Bluetooth
- Email
- Gmail
- file browsing application (for example, ASTRO File Manager or ES File Explorer)

13.1.2 Import settings

To import the settings from a file located on the device, use a file browsing application such as ASTRO File Manager or ES File Explorer, locate the settings file and choose ESET Endpoint Security.

Settings can be also imported by selecting a file in the **History** section.

13.1.3 History

History section provides you with the list of imported settings files and allows you to share, import or remove them.

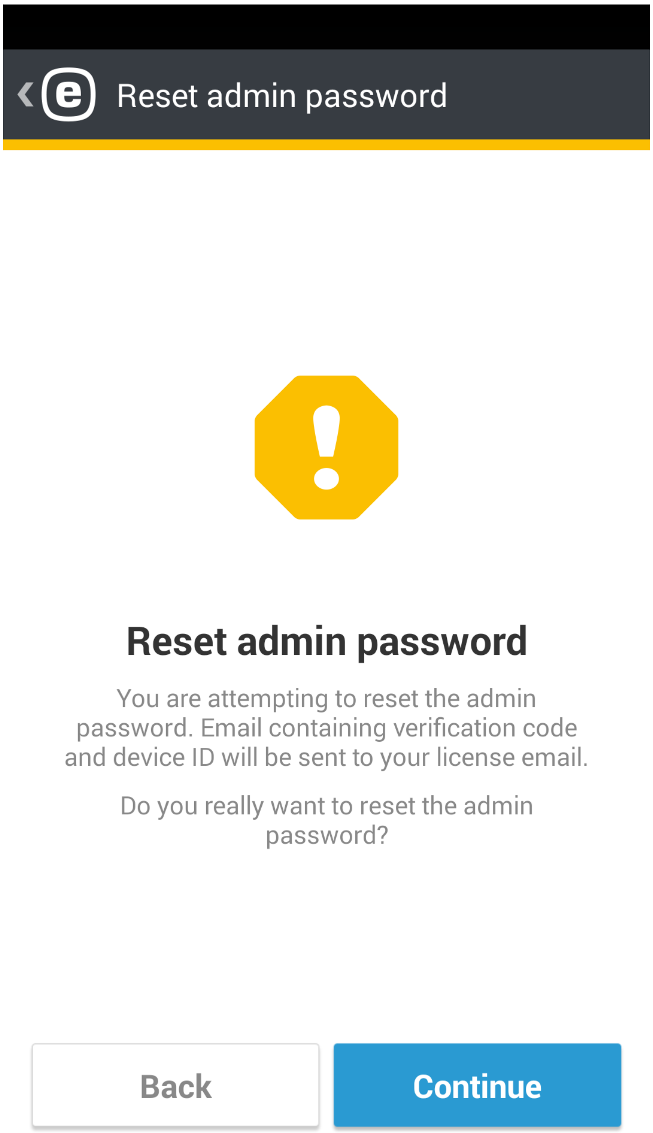
13.2 Admin Password

The **Admin password** is required to unlock a device, send Anti-Theft commands, access password protected features and uninstall ESET Endpoint Security.

IMPORTANT: Please choose the password carefully. To increase security and make the password harder for others to guess, use a combination of small letters, capital letters and numbers.

To reset the Admin password on a device with a locked screen:

1. Tap **Forgotten password?** > **Continue** > **Request verification code**. If the device is not connected to the Internet, tap the **choose offline reset** link instead and contact ESET Customer Care.
2. Check your email – an email containing verification code and device ID will be sent to the email address associated with the ESET license. The verification code will be active for 7 days after receiving.
3. Enter the verification code and a new password on your device's locked screen.



Reset admin password

Reset admin password

You are attempting to reset the admin password. Email containing verification code and device ID will be sent to your license email.

Do you really want to reset the admin password?

13.3 Remote administrator

ESET Remote Administrator (ERA) allows you to manage ESET Endpoint Security in a network environment from one central location.

Using ERA not only increases your level of security, but also provides ease-of-use in the administration of all ESET products installed on client workstations and mobile devices. Devices with ESET Endpoint Security can connect to ERA using any type of internet connection—WiFi, LAN, WLAN, Cellular Network (3G, 4G LTE, HSDPA, GPRS), etc.—as long as it is a regular internet connection (without a proxy or firewall) and both endpoints are configured correctly.

When connecting to ERA over a cellular network, a successful connection depends on the mobile network provider and requires a full-featured internet connection.

To connect a device to ERA, add the device to the **Computers** list in ERA Web Console, enroll the device using the **Device Enrollment** task and enter the **MDC Server Address**.

The enrollment link (MDC Server Address) uses the standard format `https://MDCserver:port/token` in ERA 6.4 or later. Earlier versions of ERA do not use the token parameter, so the enrollment link will use the format `https://MDCserver:port`. The link contains the following values:

- **MDCserver** – The full DNS name or public IP address of the server running Mobile Device Connector (MDC). Hostname can only be used if you are connecting through an internal Wi-Fi network.
- **Port** – The port number used to connect to Mobile Device Connector
- **Token** – The string of characters generated by admin in ERA Web Console (used only in ERA 6.4 and later)

To learn more about how to manage your network using ESET Remote Administrator, refer to the following online help topics:

- How to manage policies
- How to create client tasks
- Learn about reports

13.4 Device ID

Device ID helps the admin to identify your device in case it is lost or stolen.

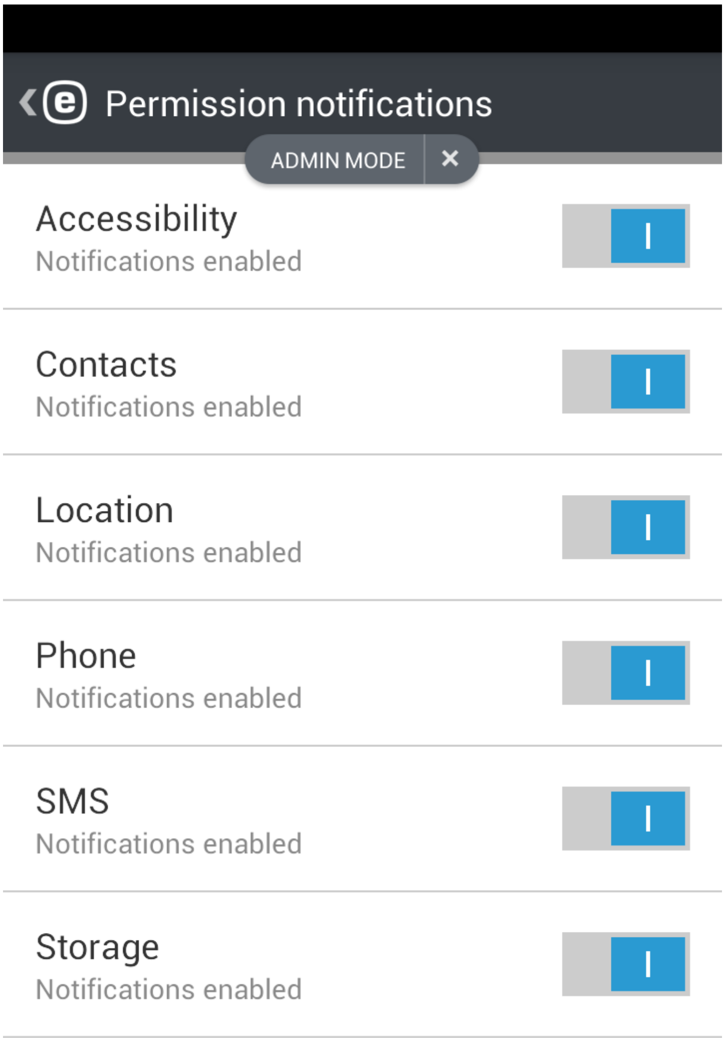
13.5 Permission management

In Android 6 (Marshmallow), Google introduced a new Permission Management and ESET Endpoint Security is compatible with it. Apps designed for Android 6.0 will ask for permissions once you start using them. Instead of giving an app access during installation, you'll be prompted the first time the app wants to access a particular device function.

ESET Endpoint Security requires access to the following functions:

- **Accessibility** - this permission is required for the proper functionality of ESET Anti-Phishing
- **Contacts** - is required for Anti-Theft and SMS & Call Filter
- **Location** - Anti-Theft
- **Phone** - Anti-Theft and SMS & Call Filter
- **SMS** - Anti-Theft and SMS & Call Filter
- **Storage** - Antivirus and Anti-Theft

Admin is allowed to disable monitoring of these permissions in **Settings** > **Permission notifications**.



Accessibility
Notifications enabled

Contacts
Notifications enabled

Location
Notifications enabled

Phone
Notifications enabled

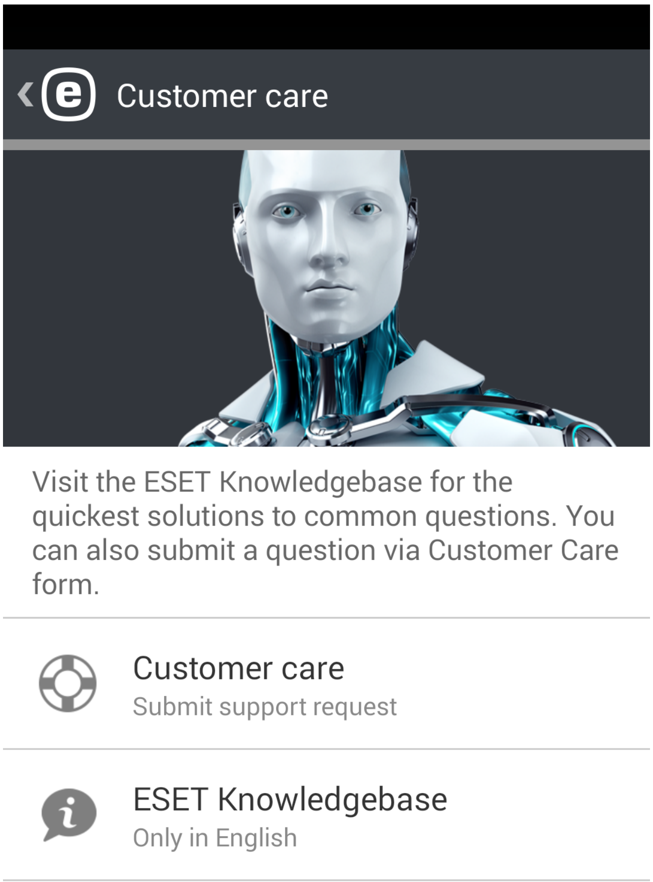
SMS
Notifications enabled

Storage
Notifications enabled

14. Customer Care

ESET Customer Care specialists are available to provide administrative assistance or technical support related to ESET Endpoint Security or any other ESET product.

To send a support request directly from your device, tap the Menu icon ⋮ in the ESET Endpoint Security main screen (or press the **MENU** button on your device), tap **Customer care** > **Customer care** and fill in all required fields.



Customer care

Visit the ESET Knowledgebase for the quickest solutions to common questions. You can also submit a question via Customer Care form.

Customer care
Submit support request

ESET Knowledgebase
Only in English

ESET Endpoint Security includes advanced logging functionality to help diagnose potential technical issues. To provide ESET with a detailed application log, make sure that **Submit application log** is selected (default). Tap **Submit** to send your request. An ESET Customer Care specialist will contact you at the email address you provided.